



Allegato

DISCIPLINA DEL TRASFERIMENTO DI DATI PERSONALI TRA LE AUTORITÀ COMPETENTI DI CUI ALL'ACCORDO TRA IL GOVERNO DELLA REPUBBLICA ITALIANA ED IL GOVERNO DELLA REPUBBLICA DEMOCRATICA SOCIALISTA DELLO SRI LANKA SUL RECIPROCO RICONOSCIMENTO DELLE PATENTI DI GUIDA AI FINI DELLA CONVERSIONE

Considerati l'art. 46 (2) (a) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati) e le garanzie previste dalla Legge sulla Protezione Dati Personali n. 9 del 2022 dello Sri Lanka, che regola il trattamento dei dati personali,

Ciascuna "Autorità competente" di una Parte Contraente (in seguito Autorità), di cui all'articolo 6 dell'Accordo tra il Governo della Repubblica Italiana ed il Governo della Repubblica Democratica Socialista dello Sri Lanka relativo al riconoscimento reciproco ai fini della conversione delle patenti di guida (in seguito Accordo), applicherà le garanzie specificate nelle clausole del presente allegato per il trasferimento di dati personali ad un'Autorità competente dell'altra Parte.

Tali garanzie sono vincolanti per le Parti e prevalgono su eventuali obblighi confliggenti esistenti nei rispettivi ordinamenti.

I. Definizioni

Ai fini delle presenti clausole s'intende per:

- (a) **"dati personali"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato") ai sensi dell'Accordo. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come un nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo in rete o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- (b) **"dati particolari"**: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici o biometrici intesi ad identificare in modo univoco una persona fisica, nonché dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona;
- (c) **"dati penali"**: dati personali relativi a condanne penali e reati o connesse misure di sicurezza;
- (d) **"dati comuni"**: dati personali che non sono particolari oppure penali;
- (e) **"trattamento"**: qualsiasi operazione o insieme di operazioni compiuti su dati personali, con o senza l'ausilio di processi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- (f) **"trasferimento"**: invio di dati personali da un'Autorità di una Parte ad un'Autorità dell'altra Parte;
- (g) **"comunicazione ulteriore"**: invio di dati personali da un'Autorità ricevente a un terzo dello stesso paese;
- (h) **"trasferimento ulteriore"**: invio di dati personali da un'Autorità ricevente a un terzo in un paese diverso dalle Parti;
- (i) **"profilazione"**: qualsiasi trattamento automatizzato di dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti personali relativi a una persona fisica.
- (j) **"violazione di dati personali"**: violazione di sicurezza che comporta accidentalmente o in

- modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati;
- (k) **"requisiti di legge applicabili"**: il quadro normativo vigente applicabile a ciascuna Istituzione, ivi compresa la normativa sulla protezione dei dati personali;
- (l) **"Autorità di controllo"**¹: l'autorità pubblica indipendente istituita dalla Parte italiana per sorvegliare l'applicazione della normativa nazionale sulla protezione dei dati personali e l'Autorità Protezione Dati dello Sri Lanka stabilita in base all'art. 28 della Legge sulla Protezione Dati Personali n. 9 del 2022
- (m) **"diritti degli Interessati"**:
- i. **"diritto a ricevere informazioni"**: il diritto di un Interessato a ricevere informazioni sul trattamento di dati personali che lo riguardano in forma concisa, trasparente, intelligibile e facilmente accessibile;
 - ii. **"diritto di accesso"**: il diritto di un Interessato di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai propri dati personali ed alle caratteristiche del trattamento in corso;
 - iii. **"diritto di rettifica"**: diritto di un Interessato di ottenere la rettifica o l'integrazione dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo;
 - iv. **"diritto di cancellazione"**: il diritto di un Interessato di ottenere la cancellazione dei propri dati personali quando i dati sono stati raccolti o trattati illecitamente rispetto alle presenti clausole ed ai requisiti di legge applicabili;
 - v. **"diritto di opposizione"**: il diritto di un Interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento di dati personali che lo riguardano, fatti salvi i casi in cui esistano motivi legittimi cogenti per il trattamento che prevalgono sugli interessi avanzati dall'Interessato, tra cui l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - vi. **"diritto di limitazione del trattamento"**: diritto di un Interessato alla limitazione del trattamento dei propri dati personali quando questi siano inesatti, il trattamento sia illecito, un'Istituzione non necessiti più i dati personali rispetto alle finalità per le quali furono raccolti oppure l'Interessato sia in attesa della valutazione di una sua richiesta di opposizione;
 - vii. **"diritto di non essere sottoposto a decisioni automatizzate"**: il diritto di un Interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Non rientrando tra le finalità dell'Accordo, è vietato lo scambio di **"dati penali"**, nonché la **"profilazione"** degli interessati, intesa come qualsiasi trattamento automatizzato di dati personali mirante a valutare determinati aspetti personali dei richiedenti la conversione della patente. Per le finalità dell'Accordo è, altresì, escluso il ricorso a procedure automatizzate.

II. Ambito di applicazione

Le presenti clausole si applicano ai titolari di patenti di guida, di cui all'articolo 1 dell'Accordo, che chiedono la conversione della patente rilasciata da una Parte in una patente rilasciata dall'altra Parte. Prima del rilascio di quest'ultima patente, gli interessati possono revocare in qualsiasi momento il consenso al trattamento dei propri dati personali, con conseguente annullamento della procedura di conversione.

Per l'accertamento del diritto e l'erogazione del servizio saranno trattati i seguenti dati personali degli interessati:

¹ In Italia l'Autorità di controllo indipendente, ai sensi dell'art. 77 dell'RGPD (UE) 2016/679, è il Garante per la protezione dei dati personali, la cui attività è disciplinata dagli artt. 140-bis e successivi del Codice in materia di protezione dei dati personali (D.lgs. 196/2003 e ss.mm.ii.).

In Sri Lanka, l'autorità per la protezione dei dati personali è l'Autorità di Regolamentazione, ai sensi della parte V della Legge sulla Protezione Dati Personali n. 9 del 2022, che è l'Autorità per la Protezione Dati dello Sri Lanka i cui fini, poteri, funzioni ed obblighi sono regolamentati dalla sez. 28 alla 40 della stessa.

1. **dati comuni:** dati anagrafici (nome e cognome, nazionalità, luogo e data di nascita, residenza/domicilio), dati di contatto (telefono, e-mail), dati relativi alla patente di guida posseduta di cui si chiede la conversione - di seguito patente di guida - (numero, data di conseguimento, di rilascio e di scadenza con riferimento a ciascuna categoria, eventuale presenza di ostacoli), modalità di conseguimento della patente di guida (esami o conversione di patente rilasciata da altro Stato con individuazione di tale Stato), eventuali ulteriori dati necessari alla conversione della patente di guida qualora questa presenti anomalie relative alla validità, all'autenticità ed ai dati in essa riportati.
2. **dati particolari:** eventuali prescrizioni relative alla patente di guida anche formalizzati sotto forma di codici, connesse all'accertamento dei requisiti di idoneità psico-fisica alla guida.

III. Garanzie per la protezione dei dati personali

1. Limitazione delle finalità

I dati personali saranno trasferiti tra le Autorità al solo fine di perseguire le finalità indicate al paragrafo II. Le Autorità non effettueranno comunicazioni o trasferimenti ulteriori di dati personali per finalità diverse da quelle sopra indicate, avendo cura di acquisire garanzie appropriate affinché i trattamenti successivi siano limitati a tali finalità, tenuto conto di quanto indicato al punto III.6.

2. Proporzionalità e qualità dei dati

L'Autorità trasferente invierà esclusivamente dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trasferiti e successivamente trattati. Il trasferimento dei dati particolari è ammesso solo se risulta strettamente indispensabile per il perseguimento delle finalità dell'Accordo.

L'Autorità trasferente assicurerà che, per quanto di sua conoscenza, i dati personali che trasferisce sono esatti e, se necessario, aggiornati. Qualora un'Autorità venga a conoscenza del fatto che i dati personali che ha trasferito a un'altra Autorità sono inesatti, ne informerà l'Istituzione ricevente, che provvederà alle correzioni del caso.

3. Trasparenza

Ciascuna Autorità, nel rispetto dell'articolo 10 dell'Accordo fornirà agli interessati un'apposita informativa sulle misure che saranno adottate nel proprio ordinamento per garantire la conformità del trattamento dei dati personali alle clausole del presente allegato, con particolare riferimento a:

- (a) identità e dati di contatto del Titolare del trattamento e, ove presente, del Responsabile della protezione dei dati;
- (b) finalità, base giuridica e modalità del trattamento dei dati personali, ivi compreso il loro periodo di conservazione;
- (c) i destinatari ai quali i suddetti dati possono essere inviati come comunicazione o trasferimento ulteriore, avendo cura di precisare le garanzie previste e le ragioni dell'invio;
- (d) i diritti degli Interessati ai sensi delle presenti clausole e dei requisiti di legge applicabili, ivi incluse le modalità di esercizio di tali diritti;
- (e) le informazioni su eventuali ritardi o restrizioni applicabili con riguardo all'esercizio di tali diritti;
- (f) il diritto di presentare reclamo ad un'Autorità di controllo, precisando i relativi dati di contatto, nonché di ricorrere ad un'Autorità giudiziaria².

² In Italia, l'Autorità giudiziaria competente in materia di protezione dei dati personali, ai sensi dell'art. 79 dell'RGPD, è il Giudice ordinario, come previsto dall'art. 152 del Codice in materia di protezione dei dati personali (D.lgs. 196/2003 e ss.mm.ii.).

In Sri Lanka, l'Autorità di Regolamentazione per la protezione dei dati personali ai sensi della Legge sulla Protezione dei Dati Personali n. 9 del 2022, è l'Autorità per la Protezione Dati che ha le funzioni di impartire direttive a Responsabili ed Incaricati del trattamento che l'Autorità ha motivo di ritenere abbiano svolto attività di trattamento in violazione della Legge.

Ciascuna Autorità diffonderà la suddetta informativa sul proprio sito, unitamente all'Accordo. Una copia dell'informativa sarà altresì inserita nelle comunicazioni individuali agli Interessati, così come un rinvio al predetto sito.

4. Sicurezza e riservatezza

Ciascuna Autorità metterà in atto misure tecniche e organizzative adeguate per proteggere i dati ricevuti da accessi accidentali o illegali, distruzione, perdita, alterazione o divulgazione non autorizzata. Le suddette misure includeranno adeguate misure amministrative, tecniche e fisiche di sicurezza. Queste misure dovranno comprendere la classificazione dei dati personali in comuni e particolari, la limitazione dei soggetti ammessi ad accedere ai predetti dati, l'archiviazione sicura degli stessi dati in funzione della loro tipologia e l'adozione di politiche volte ad assicurare che i dati personali siano mantenuti sicuri e riservati, anche ricorrendo a tecniche di pseudonimizzazione o di cifratura. Per la gestione dei dati particolari dovranno essere adottate le misure di sicurezza più rigorose, prevedendo, tra l'altro, accessi maggiormente selettivi e la formazione specialistica degli addetti.

Qualora un'Autorità ricevente venga a conoscenza di una violazione di dati personali, ne informerà entro 48 ore l'Autorità trasferente e adotterà misure ragionevoli e appropriate per porvi rimedio e minimizzarne i possibili effetti negativi per gli Interessati, ivi inclusa la comunicazione ai predetti, senza ingiustificato ritardo, dell'avvenuta violazione, qualora questa possa comportare un rischio elevato per i loro diritti e le loro libertà.

5. Modalità per l'esercizio dei diritti

Ciascuna Autorità adotterà misure appropriate affinché, su richiesta di un Interessato, possa:

(1) confermare se tratta o meno dati personali che lo riguardano e, in caso affermativo, dare accesso a tali dati, nonché fornire informazioni sul loro trattamento, ivi incluse informazioni sulle finalità del trattamento, le categorie di dati considerate, l'origine ed i destinatari dei dati, il previsto periodo di conservazione e le possibilità di reclamo e ricorso;

(2) identificare tutti i dati personali del richiedente che ha trasferito all'altra Autorità ai sensi delle presenti clausole;

(3) fornire informazioni generali, anche sul proprio sito, in merito alle garanzie applicabili ai trasferimenti all'altra Autorità.

Ciascuna Autorità darà seguito in modo ragionevole e tempestivo a una richiesta di un Interessato riguardante la rettifica, la cancellazione, la limitazione del trattamento o l'opposizione al trattamento dei propri dati personali oppure l'esercizio del diritto a non essere sottoposto a decisioni automatizzate. I recapiti di posta ordinaria o elettronica per l'invio delle predette richieste dovranno essere indicati nell'informativa agli Interessati, di cui al punto III.3 sulla trasparenza. Un'Autorità può adottare misure appropriate, come addebitare un contributo spese ragionevole per coprire i costi amministrativi della richiesta o rifiutare di darvi seguito, se questa dovesse risultare manifestamente infondata o eccessiva.

I diritti degli Interessati possono essere limitati, in misura necessaria e proporzionata in una società democratica, per salvaguardare importanti obiettivi di interesse pubblico riconosciuti dalle Parti nello spirito di reciprocità proprio della cooperazione internazionale. Rientrano in questo ambito la tutela dei diritti e delle libertà altrui, la sicurezza nazionale, la difesa, la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, nonché lo svolgimento di una funzione di controllo, ispezione o regolamentazione connessa, anche occasionalmente, alle attività esecutive e di vigilanza delle Autorità, operanti nell'esercizio dei pubblici poteri di cui sono investite. Le predette limitazioni, da disciplinare per legge, possono permanere solo finché persiste la ragione che le ha originate.

6. Comunicazione e trasferimento ulteriore di dati personali

6.1 Comunicazione ulteriore di dati personali

Un'Autorità ricevente potrà procedere alla comunicazione ulteriore di dati personali ad un terzo solo previa autorizzazione scritta dell'Autorità trasferente e purché il terzo fornisca le

stesse garanzie previste dalle presenti clausole. Nella richiesta di autorizzazione scritta, l'Autorità ricevente dovrà fornire sufficienti informazioni sulla tipologia di dati che intende comunicare, sul terzo ricevente, nonché sulla base giuridica, le ragioni e le finalità della comunicazione.

Un'Autorità ricevente potrà procedere, in via eccezionale, alla comunicazione ulteriore di dati personali ad un terzo, senza la previa autorizzazione dell'Autorità trasferente, solo se risulti necessario per almeno uno dei seguenti motivi:

- tutela degli interessi vitali di un Interessato o di un'altra persona fisica;
- accertamento, esercizio o difesa di un diritto in sede amministrativa o giudiziaria;
- svolgimento di un'indagine o di un procedimento penale strettamente connessi alle attività per le quali i dati personali sono stati trasferiti.

Nei predetti casi, l'Autorità ricevente informerà previamente l'Autorità trasferente della comunicazione ulteriore fornendo elementi sui dati richiesti, l'organo richiedente e la pertinente base giuridica. Qualora la previa informazione configghi con un obbligo di confidenzialità, come nel caso di indagini in corso, l'Autorità ricevente dovrà informare l'Autorità trasferente dell'avvenuta comunicazione ulteriore non appena possibile. Nei predetti casi, l'Autorità trasferente dovrà tenere nota delle notifiche in questione e comunicarle alla propria Autorità di controllo su sua richiesta. L'Autorità ricevente si adopererà affinché sia contenuta la comunicazione ulteriore, senza previa autorizzazione, di dati personali ricevuti ai sensi delle presenti clausole, in particolare facendo valere tutte le esenzioni e le limitazioni applicabili.

6.2 Trasferimento ulteriore di dati personali

Un'Autorità ricevente potrà procedere al trasferimento ulteriore di dati personali ad un terzo unicamente previa autorizzazione scritta dell'Autorità trasferente e purché il terzo fornisca le stesse garanzie previste nelle predette clausole. Nella richiesta di autorizzazione scritta, l'Autorità ricevente dovrà fornire sufficienti informazioni sulla tipologia di dati che intende comunicare, sul terzo ricevente, nonché sulla base giuridica, le ragioni e le finalità del trasferimento ulteriore.

7. Durata di conservazione dei dati

Le Autorità conserveranno i dati personali per il tempo previsto dai requisiti di legge applicabili, i quali dovranno prevedere un arco temporale non superiore a quello necessario e proporzionato in una società democratica per le finalità per le quali i dati sono stati trattati.

8. Tutela amministrativa e giudiziaria

Se un Interessato ritiene che un'Autorità non abbia rispettato le garanzie previste nelle presenti clausole o che i suoi dati personali siano stati oggetto di trattamento illecito, egli ha il diritto di presentare reclamo ad un'Autorità di controllo e di ricorrere dinanzi ad un'Autorità giudiziaria, in conformità ai requisiti di legge applicabili nella giurisdizione in cui è stata compiuta la presunta violazione. L'interessato ha, altresì, il diritto al risarcimento degli eventuali danni subiti.

In caso di controversia o pretesa avanzata da un Interessato nei confronti dell'Autorità trasferente, dell'Autorità ricevente o di entrambe le Autorità con riguardo al trattamento dei dati personali dell'Interessato, le Autorità si daranno reciproca informazione di tali controversie o pretese e si adopereranno per risolvere la controversia o la pretesa in via amichevole in modo tempestivo.

Qualora un Interessato sollevi un rilievo e l'Autorità trasferente ritenga che l'Autorità ricevente non abbia agito compatibilmente con le garanzie previste nelle presenti clausole, l'Autorità trasferente sospenderà il trasferimento di dati personali all'Autorità ricevente fino a quando non riterrà che quest'ultima abbia risolto la problematica in modo soddisfacente.

L'Autorità trasferente informerà sugli sviluppi della questione l'Interessato e la propria Autorità di controllo.

IV. Vigilanza

1. La vigilanza esterna sulla corretta applicazione delle presenti clausole è assicurata dalle Autorità di controllo delle due Parti.
2. Ciascuna Autorità condurrà periodiche verifiche delle proprie politiche e procedure in attuazione delle presenti clausole e della loro efficacia. A fronte di una ragionevole istanza da parte di una Autorità, l'Autorità interpellata riesaminerà le proprie politiche e procedure di trattamento dei dati personali per accertare e confermare che le garanzie previste nelle presenti clausole siano state efficacemente attuate. Gli esiti del riesame saranno comunicati all'Autorità che ha chiesto il riesame.
3. Qualora un'Autorità ricevente non sia in grado, per qualunque motivo, di attuare efficacemente le garanzie previste nelle presenti clausole, ne informerà senza ritardo l'Autorità trasferente, nel qual caso questa sospenderà temporaneamente il trasferimento di dati personali all'Autorità ricevente fino a quando quest'ultima non confermerà di essere nuovamente in grado di agire compatibilmente con le predette garanzie. Al riguardo, l'Autorità ricevente e quella trasferente terranno informate le rispettive Autorità di controllo.
4. Qualora un'Autorità trasferente ritenga che un'Autorità ricevente non abbia agito in modo compatibile con le garanzie previste nelle presenti clausole, l'Autorità trasferente sospenderà il trasferimento di dati personali all'Autorità ricevente fino a quando non riterrà che quest'ultima abbia risolto la questione in modo soddisfacente. Al riguardo, l'Autorità trasferente terrà informata la propria Autorità di controllo.

V. Revisione e vigenza delle clausole

1. Le Parti possono consultarsi per rivedere i termini delle presenti clausole in caso di cambiamenti sostanziali nei requisiti di legge applicabili. Per la modifica delle clausole, si applica la disciplina di cui all'art. 11, paragrafo 4.
2. Tutti i dati personali già trasferiti ai sensi delle presenti clausole continueranno a essere trattati applicando le garanzie ivi previste, anche dopo la scadenza dell'Accordo oppure dopo la denuncia dello stesso effettuata ai sensi dell'art. 11, paragrafo 5.





Annex

REGULATION ON THE TRANSFER OF PERSONAL DATA BETWEEN COMPETENT INSTITUTIONS OF THE AGREEMENT BETWEEN THE ITALIAN REPUBLIC AND THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA ON THE MUTUAL RECOGNITION OF DRIVING LICENSES FOR EXCHANGE PURPOSES

Having regard to Art. 46(2)(a) of the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and safeguards envisaged in Data Protection Act No: 9 of 2022 of Sri Lanka which provides for the regulation of processing personal data.

Each "Competent Authority" of one of the Parties (hereinafter referred to as "Authority"), under the Art. 6 of the Agreement between the Italian Republic and the Democratic Socialist Republic of Sri Lanka on the mutual recognition of driving licenses for exchange purposes (hereinafter referred to as "the Agreement"), shall apply the guarantees on the transfer of personal data from a Competent Institution of the other Party as specified in the Clauses of this Annex.

Such guarantees are binding for the Parties and prevail over possible conflicting requirements included in their respective legislations.

I. Definitions

For the purposes of these Clauses, the following definitions shall apply:

- (a) **"personal data"**: any information relating to an identified or identifiable natural person ("data subject"), under the Agreement. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (b) **"special categories of data"**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic or biometric data for the purpose of uniquely identifying a natural person, as well as data concerning health or a natural person's sex life or sexual orientation.
- (c) **"criminal offence data"**: personal data relating to criminal convictions and offences or related security measures.
- (d) **"ordinary personal data"**: personal data other than special categories of data or criminal offence data.
- (e) **"processing"**: any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- (f) **"transfer"**: sending of personal data by an Institution of one of the Parties to an Institution of the other Party.
- (g) **"further communication"**: sending of personal data by a receiving Institution to a third party of the same country.
- (h) **"further transfer"**: sending of personal data by a receiving Institution to a third party of a country other than the Parties (to this Agreement).
- (i) **"profiling"**: any automated processing of personal data to evaluate certain aspects related to a natural person.

nmf

- (j) **"personal data breach"**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, transferred, stored or processed personal data.
- (k) **"applicable legal requirements"**: the existing regulatory framework applicable to any Institution, including personal data protection regulations.
- (l) **"Supervisory Authority"**¹: the independent Authority set up by the Italian Party to supervise the application of national legislation on the protection of personal data and the Data Protection Authority of Sri Lanka established under Article 28 of the Data Protection Act No: 9 of 2022.
- (m) **"rights of data subjects"**:
 - i. **"right to receive information"**: the right of a data subject to obtain information on the processing of personal data concerning him or her in a concise, transparent, intelligible and easily accessible form;
 - ii. **"right of access"**: the right of a data subject to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, to obtain access to his/her personal data and details of the ongoing processing;
 - iii. **"right to rectification"**: the right of a data subject to obtain the rectification or integration of inaccurate personal data concerning him or her, without undue delay;
 - iv. **"right to erasure"**: the right of a data subject to obtain the erasure of his or her personal data when they are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or when the data have been unlawfully collected or processed according to these Clauses and applicable legal requirements;
 - v. **"right to object"**: the right of a data subject to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, subject to the existence of compelling legitimate grounds for the processing which override the interests of the data subject, including the establishment, exercise or defence of legal claims in court;
 - vi. **"right to restriction of processing"**: the right of a data subject to obtain the restriction of processing of her or his personal data when such data are inaccurate, the processing is unlawful, the Institution no longer needs the personal data for the purposes for which they were collected, or the data subject has lodged an opposition whose assessment is pending;
 - viii. **"right not to be subject to automated decisions"**: the right of a data subject not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her

Not falling within the scope of the Agreement, the exchange of **"criminal data"** is prohibited, as well as the **"profiling"** of the data subjects, understood as any automated processing of personal data aimed at evaluating certain personal aspects of the applicants for the conversion of the license. For the purposes of the Agreement, the use of automated procedures is also excluded.

II. Scope of Application

These clauses apply to the holders of driving licenses, referred to in article 1 of the Agreement, who request the conversion of the license issued by one Party into a license issued by the other Party. At any time, before the issuance of the latter license, the data subject can revoke the consent to the processing of the personal data, resulting in the cancellation of the conversion procedure.

To ascertain the law and provide the service, the following personal data of the data subject will be processed:

¹In Italy, the Supervisory Authority, under art. 77 of the GDPR (EU) 2016/679, is the Italian Data Protection Authority (Garante per la protezione dei dati personali), whose activity is regulated by art. 140-bis and subsequent articles of the Personal Data Protection Code (Legislative Decree 196/2003 and subsequent modifications and integrations). In Sri Lanka, the Authority for the protection of personal data is the Regulatory Authority, under Part V of the Personal Data Protection Act No: 9 of 2022, which is the Sri Lanka Data Protection Authority whose objects, powers, functions and duties are regulated by sections 28 to 40 therein.

1. **ordinary data**: personal data (name and surname, nationality, place and date of birth, residence/domicile), contact details (telephone, e-mail), data relating to the driving license for which conversion is requested - hereinafter driving license - (number, date of attainment, issue and expiration date with reference to each category, possible presence of impediments), modality to obtain the driving license (examinations or conversion of a license issued by another State with identification of that State), any additional data necessary for the conversion of the driving license if it presents anomalies relating to validity, authenticity and data reported therein.
2. **special categories data**: any requirements relating to the driving license also formalized in the form of codes, connected to the verification of the physical and mental fitness requirements to drive.

III. Guarantees for the Protection of Personal Data

1. Limitation of Purpose

Personal data shall be transferred between Institutions for the sole purpose of pursuing the purposes listed at paragraph II. The Institutions shall not communicate or transfer further personal data for purposes other than the above-mentioned ones, making sure to acquire appropriate guarantees in order for subsequent processing to be limited to said purposes, considering what prescribed at paragraph III.6.

2. Data Quality and Proportionality

The transferring Institution will only transfer personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed. Transfer of special categories of data is permitted solely if strictly necessary for pursuing the purposes of the Agreement.

The transferring Institution shall ensure that, to its knowledge, the personal data it is transferring are accurate and, if necessary, updated. In case an Institution finds out that personal data transferred to another Institution are inaccurate, it shall inform the receiving Institution, which will correct the data as needed.

3. Transparency

Each Institution, as prescribed at article 10 of the Agreement, shall provide the data subjects with a specific general information on the measures that will be adopted within its own legal system to ensure the compliance of the processing of personal data with the clauses of this annex, with particular reference to:

- (a) the identity and contact details of the Controller and, where applicable, of the Data Protection Officer;
- (b) the purpose, legal basis and modalities of personal data processing, including their storage period;
- (c) the recipients to whom such personal data can be sent through further communications or transfers, being sure of specifying the envisaged guarantees and reasons for sending the data;
- (d) the rights of data subjects according to these Clauses and applicable legal requirements, including the modalities for exercising such rights;
- (e) information on possible delays or applicable restrictions regarding the exercise of such rights;
- (f) the right to lodge a complaint with a Supervisory Authority, specifying the relevant contact details, as well the right to apply to a Judicial Authority²².

²²In Italy, the competent Judicial Authority competent for the protection of personal data, under art. 79 GDPR, is the Ordinary Judge, as provided for at art. 152 of the above-mentioned Code.

In Sri Lanka the Regulatory Authority for the protection of personal data under the Personal Data Protection Act No. 9 of 2022, is the Data Protection Authority, which has the power to issue directives on Controllers and Processors whom the Authority has reason to believe to have engaged in any processing activity in Contravention of the Act.

Each Institution shall publish the above-mentioned general information on its site, jointly with the Agreement. A copy of the general information, as well as a reference to such site, shall also be included in the individual communications.

4. Security and confidentiality

Each Institution shall implement appropriate technical and organisational measures to protect personal data received from accidental or unlawful access, destruction, loss, alteration or unauthorised disclosure. Such measures shall include appropriate administrative, technical and physical security measures. Such measures shall include classification of personal data as ordinary and special category data, limitation of the subjects admitted to access such data, secure storage of personal data depending on their type and adoption of policies intended to ensure that personal data are kept secure and confidential, also by implementing pseudonymization and encryption techniques. The strictest security measures shall be implemented for the processing of special categories of data, providing also more selective access and special training for the operators.

In case the receiving Institution becomes aware of a personal data breach, it shall inform the transferring Institution within 48 hours, and take reasonable and appropriate measures to remedy and minimise possible negative effects for the data subjects, including informing such subjects, without undue delay, of the occurrence of the breach, if it may pose a high risk their rights and freedoms.

5. Modalities for the Exercise of Such Rights

Each Institution shall implement appropriate measures, upon request of a data subject, in order to:

- (1) confirm whether or not it is processing personal data concerning him or her and, where that is the case, provide access to such data and information on their processing, including information on processing purposes, data categories being considered, the origin and recipients of the data, envisaged storage period and the possibility of filing a complaint or appeal;
- (2) identify all the applicant's personal data transferred to the other Institution under these Clauses;
- (3) provide general information, also on its own site, regarding the guarantees applicable to the transfer of data to the other Institution.

Each Institution shall act in a reasonable and timely manner on a data subject request for the rectification, erasure, processing limitation or opposition to processing of his or her personal data or for the exercise of his or her right not to be subject to automated decision-making. The mail or email addresses to file the above-mentioned requests must be specified in the general information sent to the data subjects, under paragraph III.3 on transparency. An Institution can take appropriate measures, for example charging a reasonable fee to cover the administrative costs of the request, or refusing to act on it, should such request be manifestly unfounded or excessive.

The rights of the data subjects can be limited, to an extent necessary and proportionate in a democratic society, to safeguard important objectives of public interest recognised by the Parties, in the spirit of reciprocity that characterizes international cooperation. The protection of the rights and freedoms of others, national security, defence, prevention, investigation, detection and prosecution of criminal offences, as well as the implementation of a monitoring, inspection or regulatory function connected, even occasionally, with the executive and supervisory activities of the Institutions, operating in the exercise of the official authority vested in them, fall into this scope. The aforesaid limitations, to be regulated by law, may continue to remain in place solely as long as the reason that originated them exists.

6. Communication and Further Transfer of Personal Data

6.1 Further communication of personal data

A receiving institution can proceed to the further communication of personal data to a third

party solely with the prior written approval of the transferring Institution, and if the third party provides the same guarantees provided for in these Clauses. In the written authorization request, the receiving Institution must provide sufficient information on the type of data it intends to communicate, the third recipient and the legal basis, reasons and purpose of the communication.

A receiving Institution can proceed, by way of exception, to the further communication of personal data to a third recipient without the prior authorization of the transferring Institution solely if it becomes necessary for one of the following reasons:

- the protection of the vital interests of a data subject or other natural person;
- the establishment, exercise or defence of a legal or administrative right;
- the conduct of an investigation or criminal proceedings closely connected with the activities for which they were transferred.

In the above-mentioned cases, the receiving Institution will previously inform the transferring Institution about the further communication, providing details on the data required, requesting body and pertinent legal basis. Whenever providing such previous information may conflict with a confidentiality obligation, as in the case of ongoing investigations, the receiving Institution shall inform the transferring Institution of the occurrence of the further communication as soon as possible. In the above-mentioned cases, the transferring Institution must keep note of these notifications and communicate them to its Supervisory Authority on its request. The receiving Institution will seek to ensure the containment of the further communication, without previous authorization, of personal data received under these Clauses, in particular by invoking all the applicable exemptions and limitations.

6.2 Further Transfer of Personal Data

A receiving institution can proceed to the further transfer of personal data to a third party solely with the prior written approval of the transferring Institution, and if the third party provides the same guarantees provided for in these Clauses. In the written authorization request, the receiving Institution must provide sufficient information on the type of data it intends to communicate, the third recipient and the legal basis, reasons and purpose of the further transfer.

7. Duration of Data Retention

The Institutions shall retain personal data for the time provided for in the applicable legal requirements, which must provide for a period of time proportionate to and no longer than necessary in a democratic society for the purposes for which they were processed.

8. Administrative and Judicial Supervision

If a data subject deems that an Institution has failed to meet the guarantees provided for in these Clauses, or his or her personal data have been subject to unlawful processing, he or she has the right to lodge a complaint with a Supervisory Authority and to apply to a Judicial Authority, in accordance with the legal requirements applicable in the jurisdiction where the presumed breach has occurred. Moreover, the data subject has the right to recover possible damages incurred.

In the event of a legal dispute or claim made by the data subject against the transferring Institution, the receiving Institution or both Institutions with regard to the processing of the personal data of such Subject, the Institutions will reciprocally exchange information on such disputes or claims and shall seek to settle the dispute or claim amicably and timely.

If the data subject raises an objection and the transferring Institution deems the receiving Institution has not acted in compliance with the guarantees provided for in these Clauses, the transferring Institution shall suspend the transfer of personal data to the receiving Institution until it will deem the latter has solved the problem satisfactorily. The transferring Institution shall inform the data subject and Supervisory Authority about the development of

the events.

IV. Supervision

1. The external supervision on the correct implementation of these Clauses is guaranteed by the Supervisory Authorities.
2. Each Institution shall conduct regular checks on its own policies and procedures in the implementation of these Clauses and their effectiveness. In response to a reasonable request by an Institution, the requested Institution shall review its policies and procedures on personal data processing to ascertain and confirm that the guarantees provided for in these Clauses have been effectively implemented. The outcome of the review shall be communicated to the Institution which requested the review.
3. If a receiving Institution is unable, for any reason, to implement effectively the guarantees provided for in these Clauses, it shall inform the transferring Institution, in which case such Institution shall suspend the transfer of personal data to the receiving Institution until the latter confirms to be again able to behave in accordance with the above-mentioned guarantees. In this regard, the receiving and transferring Institutions will keep their Supervisory Authorities informed.
4. If a transferring Institution deems the receiving Institution has not acted in compliance with the guarantees provided for in these Clauses, the transferring Institution shall suspend the transfer of personal data to the receiving Institution until it believes that the latter has resolved the matter satisfactorily. In this regard, the transferring Institution will keep its Supervisory Authority informed.

V. Review of these Clauses

1. The Parties may consult to amend the terms of these Clauses in case of substantial change in the applicable legal requirements. In amending the clauses, the discipline referred to in *article 11, paragraph 4* is applied.
2. All personal data already transferred under these Clauses shall continue to be processed by applying the guarantees provided, even after the expiration of the Agreement or after its denunciation pursuant to *article 11, paragraph 5*.

